CLAIMS

The following is a courtesy copy of the claims, indicating that no amendments are currently made:

1. (Previously Presented) A secure data switching node comprising:

a. a plurality of communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more respective communications ports;

c. a plurality of switching entry protection flags, corresponding to the plurality of switching entries, each of the plurality of switching entry protection flags configured with a predetermined value that determines whether each of the switching entries is protected from update; and

d. a controller executing a secure switching database update process, for at least one of the switching entries, wherein executing a secure switching database update process includes determining, from at least one of the switching entry protection flags, whether the at least one of the switching entries is protected from update and receiving a modification instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby an attempt by a hostile data network node to effect a modification of the at least one communication port of a protected switching entry is prevented when the protection flag is set, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

2. (Original) A secure data switching node as claimed in claim 1, wherein the communication ports are represented in the switching entries via port identifiers.

3. (Previously Presented) A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between one or more data network node identifiers and one or more of the respective physical communications ports;

c. a plurality of topology discovery disable flags corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database; and

d. a controller executing a secure data transport network topology update process for at least one of the switching entries, wherein executing a secure data transport network topology update includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database and receiving an addition instruction including a change of at least one of the respective communications ports for at least one of the data network node identifiers, whereby attempts by a hostile data network node to effect at least one addition of a switching entry specifying a communications port associated with a topology discovery disabled physical communications port are prevented, enabling the data switching node to operate securely concurrently in friendly and hostile data networking environments.

4. (Previously Presented) A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port;

c. a plurality of topology discovery disable flags, corresponding to the plurality of switching entries, each of the plurality of topology discovery disable flags configured with a predetermined value that determines whether additional switching entries are prevented from being added to the switching database;

d. a global unknown destination flood control flag; and

e. a controller implementing a secure Payload Data Unit (PDU) forwarding process, the PDU forwarding process including a modification instruction including a change of at least one communication port for at least one of the data network node identifiers, a received PDU having a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset topology discovery disable flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the topology discovery disable flags, whether switching entries are prevented from being added to the switching database.

5. (Previously Presented) A secure data switching node comprising:

a. a plurality of physical communications ports;

b. a switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between at least one data network node identifier and at least one of the communications ports;

c. a plurality of unknown destination flood control flags, corresponding to the plurality of switching entries, each of the plurality of unknown destination flood control flags configured with a predetermined value that determines whether replication of Payload Data Unit (PDU) to communication ports is prevented; and

d. a controller implementing a secure Payload Data Unit (PDU) forwarding process, wherein implementing a secure Payload Data Unit (PDU) forwarding process includes determining, from at least one of the unknown destination flood control flags, whether replication of PDU to communication ports is prevented, the PDU forwarding process further including receiving a modification instruction including a change of at least one of the communication ports for at least one of the data network node identifiers, whereby a received PDU having as a destination data node identifier not stored in the switching database is replicated only to physical communications ports having reset unknown destination flood control flags preventing hostile data network nodes connected thereto from listening to unknown destination data traffic.

6. (Previously Presented) A method of securely updating a switching database of a data switching node forwarding data traffic in a data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network identifier as a key, the switching database including a field for indicating a predetermined value associated with the source data network node identifier configured to indicate whether a new switching entry is prevented from being added to the switching database;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier does not prevent entry to the switching database; and

e. modifying the communications port specification of a switching entry found to correspond to the extracted source data network node identifier, if a switching entry protection flag associated with the found switching entry is reset whereby preventing a redirection of data traffic processed by the data switching node.

7. (Previously Presented) A method of securely updating data transport network topology information held in a switching database of a data switching node associated with the data transport network, the method comprising steps of:

a. extracting a source data network node identifier from data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries, each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with a topology discovery disable flag configured to indicate whether switching entries are prevented from being added to the switching database; and

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. adding a new switching entry to the switching database if a switching entry corresponding to the source data network node identifier is not found in the switching database and the topology discovery disable flag is reset whereby a hostile data network node is prevented from connecting to the source physical communications port.

8. (Original) A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with the source communications port.

9. (Original) A method as claimed in claimed in claim 7, wherein the topology discovery disable flag is associated with all physical communications ports of the data switching node.

10. (Previously Presented) A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with a global unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. replicating the received data traffic to each one of a plurality of physical communications ports of the data switching node if the global unknown destination flood control flag associated with the data switching node is reset; and

e. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having a topology discovery disable feature set if the global unknown destination flood control flag is set whereby a hostile data network node connected to a physical communications port having the topology discovery disable flag set is prevented from spying on unknown destination data traffic.

11. (Original) A method as claimed in claim 10, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replications of the data traffic to the source communications port.

12. (Original) A method as claimed in claim 10, wherein each physical communications port further includes an associated unknown destination flood control bit, the method further comprising a step of: suppressing the replication of the data traffic to communications ports having the associated unknown destination flood control bit set.

13. (Previously Presented) A secure method of forwarding data traffic having a destination unknown to a data switching node, the method comprising steps of:

a. extracting a source data network node identifier from the unknown destination data traffic received on a source physical communications port of the data switching node;

b. querying the switching database having a plurality of switching entries each one of the plurality of switching entries specifying an association between a data network node identifier and a communications port, the query using the extracted source data network node identifier as a key, the switching database including a field for indicating a predetermined value associated with an unknown destination flood control flag configured to indicate whether replication of PDU to communication ports is prevented;

c. receiving a modification instruction including a change of the communication port for the data network node identifier;

d. replicating the received data traffic to each one of a plurality of communications ports of the data switching node if the unknown destination flood control flags associated with the physical communications ports are reset; and

d. replicating the received data traffic to each one of the plurality of physical communications ports except physical communications ports having the unknown destination flood control flag set, whereby a hostile data network node connected to a physical communications port having the associated topology discovery disable flag set is prevented from spying on unknown destination data traffic.

14. (Original) A method as claimed in claim 13, wherein replicating the unknown destination data traffic, the method further comprises a step of suppressing the replication of the data traffic to the source communications port.

15. (Previously Presented) The secure data switching node of claim 1, further comprising an alarm configured for trigger if at least one of the switching entries is protected from update.

16. (Previously Presented) The secure data switching node of claim 3, further comprising an alarm configured for trigger if switching entries are prevented from being added to the switching database.

17. (Previously Presented) The secure data switching node of claim 4, further comprising an alarm configured for trigger if switching entries are prevented from being added to the switching database.

18. (Previously Presented) The secure data switching node of claim 5, further comprising an alarm configured for trigger if replication of PDU to communication ports is prevented.

19. (Previously Presented) The method of claim 6, further comprising triggering an alarm if switching entries are prevented from being added to the switching database.

20. (Previously Presented) The method of claim 7, further comprising triggering an alarm if switching entries are prevented from being added to the switching database.